Published and Copyright (c) 1999 - 2006
All Rights Reserved

Atari Online News, Etc.
A-ONE Online Magazine
Dana P. Jacobson, Publisher/Managing Editor
Joseph Mirando, Managing Editor
Rob Mahlert, Associate Editor

Atari Online News, Etc. Staff

Dana P. Jacobson -- Editor
Joe Mirando -- "People Are Talking"
Michael Burkley -- "Unabashed Atariophile"
Albert Dayes -- "CC: Classic Chips"
Rob Mahlert -- Web site
Thomas J. Andrews -- "Keeper of the Flame"

With Contributions by:

Fred Horvat

To subscribe to A-ONE, change e-mail addresses, or unsubscribe, log on to our website at: www.atarinews.org and click on "Subscriptions".
OR subscribe to A-ONE by sending a message to: dpj@atarinews.org and your address will be added to the distribution list.
To unsubscribe from A-ONE, send the following: Unsubscribe A-ONE
Please make sure that you include the same address that you used to subscribe from.

To download A-ONE, set your browser bookmarks to one of the following sites:

http://people.delphiforums.com/dpj/a-one.htm
http://www.icwhen.com/aone/
http://a1mag.atari.org
Now available:
http://www.atarinews.org

Visit the Atari Advantage Forum on Delphi!
http://forums.delphiforums.com/atari/

=~=~=~=

~ 20 Years of PC Viruses ~ People Are Talking! ~ CCAG 2006 Show!

~ Censored China Site! ~ Botnet Hacker Pleads! ~ LA Sues Over GTA!
~ Nyxem Worm Kills Files ~ MS Gets EU Extension! ~ AOL Beats Spammer!
~ E-Filers: No Freebies! ~ UN Backs $100 Laptop! ~ Maryland Spam Law!

-* Spyware Scam Suit Is Filed! *-
-* Site Embarrasses Spyware Purveyors! *-
-* Gates' Death-of-Spam Prediction Premature? *-

=~=~=~=

->From the Editor's Keyboard "Saying it like it is!"
"""""""""""""""""""""""""""""

And that was the week that was! What a week! Typically, our weather in New England has been up and down; and I'm not just referring to the temperature! One day balmy (for this time of the year), and then a couple of snowstorms. Fortunately, the snow didn't last too long although one storm dumped an unexpected seven inches of snow on us. So much for an early season round of golf!

My Falcon woes are still here. I'm putting this issue together with a second spare Falcon. Instead of a working spacebar, I have my settings configured so that my tab key will work semi-well as a replacement. It's a real pain in the donkey, but it will have to suffice for now. The only hard drive still connected that works is my Syquest 44. Odd, since I originally hooked that drive up as a convenient back-up drive! If I get the time, and nerve, maybe I'll venture inside the Falcon and see if I can fix it. I've taken apart numerous 520s over the years, but never a Falcon. Then maybe I'll take up one of the offers I've had for a new hard drive to connect. I really shouldn't complain - these machines have served me faithfully for almost 15 years now! And there's no way that I'm ready to retire these machines and resort solely on my PCs.

Until next time...

=~=~=~=

->A-ONE User Group Notes! - Meetings, Shows, and Info!
"""""""""""""""""""""""""""

CCAG Show 2006

It's a new year which means a new CCAG Show!

Buy, sell, trade, play, and see classic video games, computers, peripherals, memorabilia, and more at the Classic Computing and Gaming Show (CCAG) on May 27, 2006 (and again in October, 2006) at the National Guard

Armory, 3520 Grove Ave. Lorain, Ohio from 5:00 PM - 9:00 PM. Vendors, clubs, and collectors will be displaying and selling their retrogaming and retrocomputing goods, from Pong and Atari to Nintendo, Apple and IBM to Commodore and everything in between with many set up for you to play with and explore. We have 5000+ square feet of space. Help us fill it all up!

For more information please go to http://www.ccagshow.com/

=~=~=~=

PEOPLE ARE TALKING
compiled by Joe Mirando
joe@atarinews.org

Hidi ho friends and neighbors. This week's column is going to be a short one, since I've been touched by the stomach flu for the past day or two.

Didn't this stuff used to be much easier to deal with when we were younger? I seem to remember that I could shake things like this off fairly easily 'back in the day'.

Of course, they say that the memory is the second thing to go. Unfortunately, I don't remember what the FIRST was. <grin>

There seems to be a slight shortage of UseNet messages this week... maybe everyone else has the stomach bug too... so, this is going to be a short-ish column for two reasons.

So without further delay, let's take a look at what's going on with the UseNet.

From the comp.sys.atari.st NewsGroup
==========

Joe Iron tells us:

"I've just obtained Papyrus from Ebay. A couple of questions:
- How can I backup the original disks?
- Does anybody have the RSC files translated to English?"

Edward Baiz asks Joe:

"What version do you have? I have and use version X. I thought there was some English versions of the RSC files on the Net, but I am not positive."

Martin Elsässer asks Edward:

"A little question: I found a problem in Papyrus X when using the options for the dialogues. Papyrus crashes and freezes my PowerBook (MacOS 8.6

with MagiCMac 6.2) when saving the changed options for the "dialog". With MacOS X and MagiCMacX Papyrus doesn't crash, but the options "dialog" can not be called from the menu directly. What happens, if you change the behavior of the dialogs for the buttons "OK", "Cancel" vs. "Accept", "Back" and save these changes?"

Martin Tarenskeen adds:

"I got Papyrus X from 16/32 systems
(http://www.1632-sales.zenwebhosting.com)
English!"

'Chris' asks about the ST's parallel interface:

"Was thinking back to the good old days of controlling stuff from the parallel port. I know years ago I did a 12x6 led array which was controlled from STOS, just using the LPRINT command to control address/data levels on the led matrix.

Was thinking of a small plug in box which would plug into the parallel port, will house some LED's for a indication that the port is active, then offering either a larger LED matrix box, or another box for controlling mains equipment etc, anything is possible really. The parallel interface will become the "host interface", which will decode commands and give probably a output set of 16 ports. Could even be used on the PC, even though most have gone USB now anyway.

Was half thinking aloud about this since its something I've had in mind for a while now, so just seeing if they would be any interest in doing a small production run of the things. The host itself isn't going to cost much to build and develop so its going to be pretty cheap *I think*. Depending on what people are wanting to control then it depends on cost of building some form of "output box", either holding power mosfets for controlling 12V motors/lamps etc, or relays for controlling mains equipment.

Was just a though about if there would be interest in it, controlling stuff from computers is always fun."

Ronald Hall tells Chris that it...

"Reminds me of the "Robotic" kit that sold for the ST for awhile, or the X10 stuff that controls household appliances.

I'd be interested in a modern version that would run on all Atari models. What about software?"

Chris tells Ronald:

"I can do software but it can only be in STOS, which unfortunately will not run in any multi-os. I could publish the control docs for it should there be anyone who would want to write software for it... Will have to see if I can find someone before I consider the hardware as I think it could become problematic having being limited on one program running."

Joe Iron now asks about...

"Where to download the latest (1.16.3) Mint kernel from?
Atari-Source.org always denies to access the files."

Our buddy Lonny Pursell tells Joe:

"http://sparemint.atariforge.net/sparemint/mint/kernel/1.16.1/"

Odd Skancke adds:

"Yes, this will get you the latest 1.16.1 beta release. If you haven't installed MiNT before, I would do the following;

1. Install EasyMiNT
2. Get the 1.16.1 beta at the above link, read the docs on how to upgrade an EasyMiNT installation.
3. Get the latest alpha release from xaaes.atari.org, it contains the current 1.16 kernel, 1.16.cur. "

Mark Duckworth tells Odd:

"Yeah, this is a better solution for the newbie. But in a little bit the atari-source.org problems should be fixed. Someone needs to tell me this stuff."

Florent Gilles asks about a Dungeon Master clone:

"Does anyone remember an ST Demo witch included a nice Dungeon Master clone?"

Mickael Pointier interjects:

"The Phaleon GigaDemo perhaps ?
http://www.defence-force.org/computing/atari/demos/index.htm "

Florent replies:

"Maybe, but how can I access to the Dungeon Master Menu in this demo?

Ok, I've found it but that's not the DM Menu selector of the Phaleon. The DM clone I'm talking about has huge levels and wrap zones were filed with sort of transparent blue walls."

Well folks, that's it for this time around. Tune in again next week, same time, same station, and be ready to listen to what they are saying when...

PEOPLE ARE TALKING

=~=~=~=

->In This Week's Gaming Section - 'Marc Ecko's Getting Up
Street Fighter Alpha!
LA Sues Over GTA Game!

=~=~=~=

->A-ONE's Game Console Industry News - The Latest Gaming News!

Atari and Marc Ecko Announce 'Marc Ecko's Getting Up:
Contents Under Pressure' Goes Gold

Atari, Inc. and Marc Ecko, the visionary behind several of today's most respected youth lifestyle brands, Tuesday announced that Marc Ecko's Getting Up: Contents Under Pressure has gone gold and is on schedule to ship to stores nationwide on February 14 in North America and on February 17 in Europe.

Set in the city of New Radius, Marc Ecko's Getting Up: Contents Under Pressure features a world where freedom of expression is suppressed by a tyrannical city government. In the game, players assume the role of Trane - an unlikely hero just looking to get up until he realizes there is much more at stake. Gamers learn and master various graf skills, starting as a toy (beginner) graffiti artist and using street-smarts, athletic prowess and vision necessary to become an "All City King," the most reputable of all graffiti artists. During their quest, players risk their lives navigating vertical landscapes while battling rival crews, a corrupt Mayor and the city's Civil Conduct Keepers (CCK) all in an effort to reach the sweet spots of New Radius, where a well-placed tag brings respect and reputation. Gamers also find themselves with an even greater burden - to use their high-wire graffiti talents to expose the oppressive mayor and set the city free.

"Marc Ecko's Getting Up: Contents Under Pressure fuses authentic urban culture and multi-faceted gameplay in a way gamers have never seen before," said Marc Metis, senior vice president, marketing, Atari, Inc. "Consumers are looking for something new, unique, and original in gaming, and this game delivers it."

Marc Ecko's Getting Up: Contents Under Pressure includes a variety of star-studded voice talent such as renowned hip-hop artist Talib Kweli, Sean "Diddy" Combs, Rosario Dawson, Brittany Murphy, George Hamilton, Giovanni Ribisi, Adam West, Andy Dick, Charlie Murphy, The RZA and Michael "M.C. Serch" Berrin.

More than 65 graffiti artists have lent their signature tags and art to the game's urban environments, while six legendary artists - Cope 2, FUTURA, OBEY: Shepard Fairey, Seen, Smith and T-kid - have served as

in-game mentors to the game’s lead protagonist.

In addition, Atari and Mr. Ecko, through the support of Mr. Combs’ legendary A&R skills, have assembled an impressive soundtrack featuring an array of licensed music and various original tracks, including an exclusive version of Notorious B.I.G.’s "Who Shot Ya," remixed by Serj from the band System of a Down; "Clik, Clak, and Spray" from Pack FM; "Book of Judges" from Pharoahe Monch; and "Getting Up Anthem: Part 1," performed by legendary Hip- Hop artist Rakim and Talib Kweli.

Developed by The Collective, Marc Ecko’s Getting Up: Contents Under Pressure is rated ’M’ for Mature and will be available for the PlayStation2 computer entertainment system, Xbox video game and entertainment system from Microsoft, and Windows. A mobile version is currently available through Glu Mobile. For additional information about the game please visit http://www.gettingup.com.

Street Fighter Alpha Anthology For Playstation 2 Announced

You win! The ultimate in arcade brawlers comes home as Capcom announced Street Fighter Alpha Anthology for the PlayStation2 computer entertainment system, a monumental compilation of the entire Street Fighter Alpha arcade series. The collection features direct arcade conversions of StreetFighter Alpha, Street Fighter Alpha 2, Street Fighter Alpha 2 Gold and Street Fighter Alpha 3 which have never before been available together in one package. As an added bonus, the "pint-sized" Super Gem Fighter Mini Mix (also released on consoles as Pocket Fighter), is included which brings the total to five action packed games on one disc. Street Fighter Alpha Anthology is scheduled for release throughout North America in summer 2006. To date, the Street Fighter franchise has sold more than 27million units worldwide.

All titles in the collection feature three core gameplay options. Arcade mode pits competitors against a series of CPU controlled opponents in order to beat the game. Versus mode allows two players to choose among the cast of characters for intense head-to-head battles. Fighters can practice special moves and combos to hone their skills in the training mode. Additionally, all four Alpha titles feature survival mode as well as a dramatic battle mode which allows 2-on-1 tagteam matches.

Street Fighter Alpha brings together a cast of 13 characters from the collective Street Fighter universe. The series’ inaugural title introduces super combos and alpha counters to add a new dimension to fighting. Street Fighter Alpha2 ups the ante with 18 fighters and several new options including high and low Alpha counters as well as more moves and combos for each character. In addition, the second title launches the Custom Combo system which lets players use up a super meter to perform devastating multi-hit combos. Street Fighter Alpha 2 Gold is an enhanced version of the previous game featuring different versions of some of the characters. The most robust entry, Street Fighter Alpha 3, includes an unprecedented 25 characters and offers players the choice of three "isms" fighting styles made popular in previous Street Fighter games. Super Gem Fighter Mini Mix rounds out the anthology with miniature versions of popular Capcom fighters in fierce battles. Combatants vie to collect power-up gems as they perform an array of special attacks and powerful combos.

Los Angeles Sues Over ’Grand Theft Auto’ Game

The city of Los Angeles has sued Take-Two Interactive Software Inc. for selling pornographic video games to children with its best-selling game "Grand Theft Auto: San Andreas," which last year was found to have hidden sex scenes.

Shares of Take-Two plunged 13.7 percent to $14.69 on the Nasdaq - a level unseen since 2003 - after an analyst downgraded its shares to "sell" from "neutral," citing a variety of financial, operational and management risks.

Los Angeles City Attorney Rockard Delgadillo, in the suit filed on Thursday, accused the game publisher of failing to disclose the pornographic content to get the game onto shelves of major retailers that do not carry games rated "Adults Only 18+."

Delgadillo said the company further deceived consumers by first claiming that hackers had modified the original version of the games, then announcing a week later that the sex scenes were written into the original game code.

The lawsuit demands that Take-Two and Rockstar Games, the subsidiary behind "Grand Theft Auto," one of the best-selling in video game franchises history, stop marketing the games to children, pay fines and return $10 million in profits.

Last summer, the video game ratings board slapped a restrictive "adult" rating on "Grand Theft Auto: San Andreas" because of explicit sex scenes, known as "Hot Coffee," that allow players to engage in virtual sex acts.

The Entertainment Software Ratings Board launched an investigation and took the unusual step of changing the rating on the game to "Adults Only 18+" (AO) from "Mature 17+."

Take-Two had to pull the games off store shelves and repackage them with the new rating, which crimped game sales and disrupted company operations.

The lawsuit charged that Take-Two knowingly deceived the video game ratings board and flouted California law to market the game as suitable for teens, the lawsuit alleged.

The city also claims that Take-Two "marketed the ’Grand Theft Auto’ series in a fashion that encourages the creation of (software modifications), which has added to the counter-culture image of the games, enhancing their popularity and hence their profitability."

The lawsuit asks that Take-Two be ordered to disgorge the profits from the estimated 200,000 copies of the game it sold for about $10 million in California, and that it alert customers who purchased "Grand Theft Auto: San Andreas" before the ratings change about the sex scenes.

It also demands a $2,500 fine for each untrue or misleading statement the company purportedly made about the games.

Delgadillo appears to have a good case if he can prove that the scenes were embedded in the game and that the company misled the ratings board and the public, said attorney Stephen Smith, a partner at Greenberg Glusker in Los Angeles.

"It’s a pretty black and white issue. If they can prove it’s true, I think they have a claim," said Smith.

"The greatest direct risk to Take-Two is that they would have to turn over the money," said Smith, who represents a variety of video game companies including Ubisoft, but has no affiliation with Take-Two or the Los Angeles city attorney.

Consumers in New York already have sued the company over the debacle and are seeking class action status. Take-Two also disclosed in July that the Federal Trade Commission was investigating advertising claims related to the controversial game.

=~=~=~=

A-ONE’s Headline News
The Latest in Computer Technology News
Compiled by: Dana P. Jacobson

PC Virus Celebrates 20 Years of Havoc

This month marks a somewhat dubious anniversary for PC computer users: It’s the 20th anniversary of the first PC virus. First discovered in the wild in January 1986, the Brain virus inspired hordes of hackers during the 1990s and, more recently, a whole new class of online criminal.

Although the Brain virus has achieved a certain amount of notoriety as the first PC virus, its effects were not widespread because the only method by which viruses could be transmitted from one PC to another at that time was by floppy disk.

No one can pinpoint the exact time the Brain virus was created, but the most popular theory is that it was created by two engineers, named Basit and Amjad, at a software firm in Pakistan.

The virus reportedly replaced the executable code on a bootable floppy disk with the Brain code designed to infect each floppy subsequently opened on the PC.

An American computer scientist, Fred Cohen, coined the phrase "computer virus" in 1983. Cohen defined a computer virus as "a computer program that can affect other computer programs by modifying them in such a way as to include a (possibly evolved) copy of itself."

In 1990, Symantec launched Norton Antivirus, one of the first antivirus programs ever developed by a major software company. The move by Symantec spawned a new industry. In 1992, some 1,300 new viruses were created, a 420 percent increase from December 1990.

Between 1990 and 1998, the computer world suffered from all kinds of new viruses, even those that could change their appearance with each new infection to thwart antivirus software. This era also saw the birth of

e-mail-borne malware and Microsoft Word viruses. Currently, there are some 150,000 viruses circulating in the wild.

"In 20 years, viruses have moved from floppy disks to file viruses, to e-mail viruses, to Internet worms, to targeted Trojan-horse attacks," said Graham Cluley, senior security consultant at Sophos.

In the 1990s, viruses amounted mainly to electronic graffiti. Occasionally, the virus would cause financial harm, but only with regard to damage to computers. Today, viruses have become the bread and butter for a new breed of criminals and crime syndicates.

"Compared to 20 years ago, [viruses were] mostly research and experimental," said Rob Ayoub, an analyst at Frost & Sullivan. "Even when there was malicious intent, it was to prove who the better hacker was and who had the best skillset. A real key was looking for tag lines in the assembler code for the different hackers or groups."

Most security analysts say that viruses written today have a much more malicious intent. Criminals can strike individuals and businesses in several ways, whether through extortion by threatening to hit a targeted company with a denial-of-service attack or through hidden malware and keyloggers that can gather personal or corporate information and lead to identity theft and a slew of other crimes.

"With so many home users connecting to the Internet, there are many potential victims out there for the criminals to feast upon," said Cluley. "The greater connectivity has brought more opportunities for malware to spread and increased the number of potential victims."

According to Ayoub, the change in the nature of viruses reflects a change in the culture and the proliferation of technology in our daily lives. "The Internet changed how the viruses were distributed, but the driver for why it is more financial now is that [the computer] is so integrated in our daily lives," said Ayoub. "Fraud has been out their for years. Now, instead of bad checks, criminals acquire credit-card numbers online."

"FBI computer crime survey of 2,000 public and private organizations released last week found that, in 2005, nine out of 10 organizations experienced "computer security incidents."

Viruses topped the list of attacks with nearly 84 percent of respondents saying that they had been adversely affected, with spyware coming in second at just under 80 percent. The financial impact of attacks from viruses and worms accounted for some $12 million in losses out of total losses of $32 million.

While the Internet has developed into a prime avenue for hackers to distribute malicious software, it also has become a way for security vendors to neutralize viruses more quickly, particularly throught the automatic-update features in most antivirus software.

"When I first entered the antivirus industry, updates were sent out on a 5.25-inch floppy disk," Cluley remarked. "A lot has changed in that time."

Nyxem Worm Programmed to Erase Files

Antivirus vendors are warning of a rapidly-spreading worm that is carrying a potentially destructive set of instructions. The Nyxem worm - also nicknamed the Kama Sutra worm - is programmed to overwrite all of the files on computers it infects on February 3, says Mikko Hypponen, chief research officer at F-Secure.

F-Secure researchers found the worm truncates files to 20 bytes and causes an error message when one is opened, he says.

"We are expecting to see problems in two weeks' time," Hypponen says.

The worm appears to be programmed to overwrite all files on the third day of every month, Hypponen says. So far, there's no indication where Nyxem originated.

While most antivirus vendors have issued updates for their software, Nyxem is spreading quickly, and its creators have posted a counter on a Web site that records new infections. According to F-Secure's security blog, the counter was showing around 510,000 infections as of Sunday night.

Nyxem infections may be rising because it is taking advantage of computers that have already had their antivirus software disabled by some other virus such as Bagle, Hypponen says.

The worm, which is spread through e-mail, uses a dated technique to entice users by promising pornography, says Graham Cluley, senior technology consultant, at Sophos. Nyxem lacks the sophistication of recent Trojan horse-style viruses that are more targeted and less prevalent in order to evade detection, Cluley says.

Nonetheless, users appear to still be clicking, and the worm was accounting for about 35 percent of virus traffic as of Monday morning, he says.

"It's a bit of a throwback to an old trick," Cluley says.

The worm harvests e-mail addresses and then sends itself out again. The e-mail subject line may contain text that says "Miss Lebanon 2006" or "School girl fantasies gone bad," according to Sophos.

California Man Pleads Guilty to Felony Hacking

A 20-year-old hacker admitted Monday to surreptitiously seizing control of hundreds of thousands of Internet-connected computers, using the zombie network to serve pop-up ads and renting it to people who mounted attacks on Web sites and sent out spam.

Jeanson James Ancheta, of Downey, Calif., pleaded guilty in Los Angeles federal court to four felony charges for crimes, including infecting machines at two U.S. military sites, that earned him more than $61,000, said federal prosecutor James Aquilina.

Under a plea agreement, which still must be approved by a judge, Ancheta faces up to 6 years in prison and must pay the federal government restitution. He also will forfeit his profits and a 1993 BMW. Sentencing is schedule for May 1.

Prosecutors called the case the first to target profits derived from use of "botnets," large numbers of computers that hackers commandeer and marshal for various nefarious deeds. The "zombie" machines' owners are unaware that parasitic programs have been installed on them and are being controlled remotely.

Botnets are being used increasingly to overwhelm Web sites with streams of data, often by extortionists. They feed off of vulnerabilities in computers that run Microsoft Corp.'s Windows operating system, typically machines whose owners haven't bothered to install security patches.

A November indictment charged Ancheta with 17 counts of conspiracy, fraud and other crimes connected to a 14-month hacking spree that started in June 2004 and that authorities say continued even after FBI agents raided his house the following December.

"Part of what's most troubling about those who commit these kinds of offenses is they think they'll never be caught," said Aquilina, who spent more than a year investigating Ancheta and several of Ancheta's online associates who remain uncharged co-conspirators.

Ancheta's attorney, federal public defender Greg Wesley, did not immediately return phone calls seeking comment.

Ancheta has been in federal custody since his November indictment. He previously worked at an Internet cafe owned by a relative and had hoped to join the military reserves, according to his aunt, Sharon Gregorio. Court documents suggested he had a taste for expensive goods, spending $600 a week on new clothes and car parts.

The guilty plea comes less than a week after the FBI released a report that estimates viruses, worms and Trojan horse programs like the ones Ancheta employed cost U.S. organizations $11.9 billion each year.

November's 52-page indictment, along with papers filed last week, offer an unusually detailed glimpse into a shadowy world where hackers, often not old enough to vote, brag in online chat groups about their prowess in taking over vast numbers of computers and herding them into large armies of junk mail robots and arsenals for so-called denial of service attacks on Web sites.

Ancheta one-upped his hacking peers by advertising his network of "bots," short for robots, on Internet chat channels.

A Web site Ancheta maintained included a schedule of prices he charged people who wanted to rent out the machines, along with guidelines on how many bots were required to bring down a particular type of Web site.

In July 2004, he told one chat partner he had more than 40,000 machines available, "more than I can handle," according to the indictment. A month later, Ancheta told another person he controlled at least 100,000 bots, and that his network had added another 10,000 machines in a week and a half.

In a three-month span starting in June 2004, Ancheta rented out or sold bots to at least 10 "different nefarious computer users," according to the plea agreement. He pocketed $3,000 in the process by accepting payments through the online PayPal service, prosecutors said.

Starting in August 2004, Ancheta turned to a new, more lucrative method to profit from his botnets, prosecutors said. Working with a juvenile in Boca

Raton, Fla., whom prosecutors identified by his Internet nickname "SoBe," Ancheta infected more than 400,000 computers.

Ancheta and SoBe signed up as affiliates in programs maintained by online advertising companies that pay people each time they get a computer user to install software that displays ads and collects information about the sites a user visits.

Prosecutors say Ancheta and SoBe then installed the ad software from the two companies - Gamma Entertainment of Montreal, Quebec, and Loudcash, whose parent company was acquired last year by 180Solutions of Bellevue, Wash. - on the bots they controlled, pocketing more than $58,000 in 13 months.

"It's immoral, but the money makes it right," Ancheta told SoBe during one online chat, according to the indictment.

"I just hope this (Loudcash) stuff lasts a while so I don't have to get a job right away," SoBe told Ancheta during a different conversation.

Aquilina, the assistant U.S. attorney prosecuting the case, wouldn't say whether authorities plan to charge SoBe or any of the people accused of renting out Ancheta's bots, many of whom are described as "unindicted co-conspirators."

During the course of their scheme, Ancheta and SoBe infected U.S. military computers at the China Lake Naval Air Facility and the Defense Information System Agency headquartered in Falls Church, Va., according to a sworn declaration signed by Ancheta.

AOL Wins $5 Million Judgment Against Spammer

A man who sent billions of junk e-mails hawking online college degrees, sexually explicit Web sites and "generic Viagra" must pay more than $5 million in penalties to America Online, a federal judge ruled.

Christopher William Smith, of Prior Lake, Minn., was considered one of the world's worst spammers, operating under the name Rizler. He is now in jail in Minnesota awaiting trial on criminal charges that he violated federal drug laws while operating an online pharmacy.

On Tuesday U.S. District Judge Claude Hilton issued a summary judgment against Smith ordering him to pay $5.3 million in damages and $287,000 in legal fees to AOL, which filed a civil suit against Smith under the Can-Spam act.

AOL spokesman Nicholas Graham said Smith "was the poster child for the Can-Spam Act," which Congress enacted in 2004 to crack down on unsolicited junk e-mail.

"This is someone we've been pursuing for three years," Graham said. "It's one of the largest judgments we've received."

Hilton issued a summary judgment in favor of Dulles-based AOL after Smith "refused to participate in this case, willfully disregarding ... discovery obligations and failing to comply with multiple court orders," according to the judge's order.

Court records show that Smith’s lawyers withdrew from the case several months after it was filed.

In addition to e-mails promoting generic Viagra and pornographic Web sites, Smith also advertised cable TV descramblers and penis enhancement pills.

In an initial response to AOL’s lawsuit, Smith’s lawyers denied wrongdoing and questioned the constitutionality of the Can-Spam law.

Graham said that AOL has won tens of millions of dollars in judgments against more than 30 spammers under the federal law and a similar Virginia law.

Maryland Spam Law Can Be Enforced

Those annoying e-mails offering home financing deals or other offers can violate Maryland law, even if they’re sent from another state, a state appeals court has ruled.

Court of Special Appeals Judge Sally D. Adkins sided with a law student who argued that he could sue a New York e-mail marketer who had sent him advertising messages.

The decision, issued Thursday, overturns a lower court ruling that Maryland’s 2002 Commercial Electronic Mail Act was unconstitutional because it sought to regulate commerce outside state borders.

Adkins, in a 60-page decision, blasted the marketer’s claims that he should not be punished for violating Maryland law because he had no way of knowing whether his e-mails would be opened in Maryland.

"This allegation has little more validity than one who contends he is not guilty of homicide when he shoots a rifle into a crowd of people without picking a specific target, and someone dies," the judge wrote.

The courts have yet to rule on whether the marketer, Joseph M. Frevola, had indeed violated the law.

Maryland was one of the first states to try to control junk e-mail through legislation, and its 2002 law predates the 2004 federal CAN-SPAM Act. The federal law superseded most state laws unless they specifically addressed deceptive or fraudulent e-mail, which Maryland’s does.

The next step in the case is unclear. Baltimore lawyer Andrew Dansicker, who represents Frevola, said the marketer would like to appeal, but his company has since gone out of business.

Washington AG, Microsoft File Spyware Scam Suit

Washington state and Microsoft Corp. said on Wednesday they filed civil suits against a New York-based company for violating the state’s anti-spyware law and called for cooperation between technology companies and government to crack down on Internet fraud.

Washington Attorney General Rob McKenna accused Secure Computer LLC and its associates of marketing software that falsely claims a computer is infected with spyware in order to sell a program to clean the PC when in fact the software makes the computer more susceptible to attacks.

"Spyware has overtaken computer viruses as the number-one threat to personal computer users," McKenna said in a statement. "This lawsuit will make it clear to those who prey on consumers' fears about spyware that we are no longer going to tolerate their heinous activities."

Malicious spyware can often track victims' Internet activity, hijack their home pages and bombard them with pop-up ads.

The 16-count suit, filed on Tuesday in U.S. District Court in Seattle, is the first lawsuit under Washington's new computer spyware act and represents the growing cooperation between the technology sector, lawmakers and regulators to limit unwanted tracking and advertising software.

Redmond, Washington-based Microsoft said it referred this case to the attorney general's office and provided technical and forensic assistance. Microsoft also filed a parallel suit in federal court.

"Microsoft continues to collaborate with many state attorneys general to help protect computer users from the effects of spyware, spam and cybercrime, such as identity theft," said Nancy Anderson, deputy general counsel for Microsoft.

Microsoft's lawsuit also alleges Secure Computer used the software giant's trademarks to falsely suggest Microsoft sponsored or approved the ineffective Spyware Cleaner software.

Free Website To List Programs With Spyware

Here's a new way to attack spyware: embarrass its purveyors.

A free website (StopBadware.org) launching Wednesday plans to provide a list of programs that contain spyware and other malicious software. It will also identify companies that develop the programs and distribute them on the Internet.

Consumers can then decide if a program is safe to download.

"For too long, these companies have been able to hide in the shadows of the Internet," says John Palfrey, who heads the Berkman Center of Internet & Society at Harvard Law School and is spearheading the project. "What we're after is a more accountable Internet."

The initiative is being run by Harvard and the Oxford Institute and is backed by high-tech heavyweights including Google and Sun Microsystems. Consumer Reports' WebWatch is serving as a special adviser.

Spyware invades PCs without users' knowledge when they download applications such as music file-sharing programs or screen savers, or visit certain websites. Often, spyware tracks Web-surfing habits and bombards victims with related pop-up ads. More nefarious versions monitor keystrokes to steal Social Security numbers or passwords for identity theft.

Also on the hit list of the StopBadware coalition are malicious "adware" programs that serve up onslaughts of pop-up ads or software that contains hidden viruses and worms.

At least 60% of home PCs are infected with one or more of these "badware" programs, says Forrester Research analyst Natalie Lambert.

The prevalence of the programs has spawned a booming industry of anti-spyware and anti-virus software. Internet providers such as America Online and EarthLink include the software free with service. But such programs typically can’t identify all the rogue software on a PC and might not be able to eradicate a deeply embedded program even if they do, says Ferris Research analyst Fred Berlack.

By checking StopBadware.org, its organizers say, consumers can choose, in the first place, not to download a program containing the malicious software. The coalition is encouraging consumers to visit the website to log their experiences with harmful programs.

It will then use that information to compile reports on suspect programs, websites and companies that foist the software on consumers without getting their consent. The worst offenders will be spotlighted. It will take several months to gather a significant-size database, Palfrey says.

Some websites already provide information on spyware. Others identify suspect software for a fee. But the StopBadware group says it aims to be the biggest free clearinghouse.

Berlack is skeptical that many consumers will use the service. "I don’t think the average Joe has the time or inclination to check every time he opens up a new website or downloads a program," he says.

But Te Smith of consultants FFW Partners, says, "Anything that helps people be more informed is useful. I applaud these companies for using their market presence and reach to try to educate consumers."

Google Launches Censored China Site

Google Inc. launched a search engine in China on Wednesday that censors material about human rights, Tibet and other topics sensitive to Beijing - defending the move as a trade-off granting Chinese greater access to other information.

Within minutes of the launch of the new site bearing China’s Web suffix ".cn," searches for the banned Falun Gong spiritual movement showed scores of sites omitted and users directed to articles condemning the group posted on Chinese government Web sites.

Searches for other sensitive subjects such as exiled Tibetan leader the Dalai Lama, Taiwan independence, and terms such as "democracy" and "human rights" yielded similar results.

In most such cases, only official Chinese government sites or those with a ".cn" suffix were included.

Google, which has as its motto "Don’t Be Evil," says the new site aims to

make its search engine more accessible in China, thereby expanding access to information.

Yet the move has already been criticized by media watchdog Reporters Without Borders, which also has chided Yahoo Inc. and Microsoft Corp.’s MSN.com for submitting to China’s censorship regime.

"When a search engine collaborates with the government like this, it makes it much easier for the Chinese government to control what is being said on the Internet," said Julien Pain, head of the group’s Internet desk.

However, technology analyst Duncan Clark said such criticisms probably wouldn’t generate problems for Google’s business elsewhere, given weak responses to previous cooperation between foreign Internet companies and Chinese authorities.

Past incidents "haven’t seemed to gel into anything that could dissuade Google," said Clark, the managing director of Beijing-based consultancy BDA China Ltd.

Chinese Internet users said Mountain View, Calif.-based Google Inc.’s move was inevitable given Beijing’s restrictions on the Internet, which the government promotes for commerce but heavily censors for content deemed offensive or subversive.

"Google has no choice but to give up to the Party," said one posting on the popular information technology Web site PCONLINE, signed simply "AS."

Google’s move was prompted by frequent disruptions of the Chinese-language version of its search engine registered under the company’s dot-com address in the United States.

Government filtering has blocked access or created lengthy delays in response time.

Google’s senior policy counsel Andrew McLaughlin defended the new site as better serving Chinese customers.

"In deciding how best to approach the Chinese - or any - market, we must balance our commitments to satisfy the interests of users, expand access to information, and respond to local conditions," McLaughlin said in an e-mailed statement, .

McLaughlin said search results would be removed based on local laws, regulations or policies.

"While removing search results is inconsistent with Google’s mission, providing no information (or a heavily degraded user experience that amounts to no information) is more inconsistent with our mission," he said.

There was no indication that Google would disable access to its .com site within China.

McLaughlin said the company wouldn’t host its e-mail or blogging services in China that can be mined for information about users, and would inform users if information had been deleted from searches. Such messages appeared in searches for Falun Gong and other sensitive topics.

Clark said Google likely hopes to avoid the bad publicity incurred by Yahoo last year after it provided the government with the e-mail account

information of a Chinese journalist who was later convicted of violating state secrecy laws.

"They want to avoid those kinds of headlines," he said.

Google hopes the move will shore up its competitiveness against both foreign competitors such as Yahoo and domestic ones like Baidu.com Inc., a Beijing-based company in which Google owns a 2.6 percent stake. Baidu.com is currently China's most popular search engine.

China has more than 100 million Web surfers and the audience is expected to swell.

Wang Lijian, a spokesman for China's Ministry of Information Industry which oversees Internet licensing, said he had not heard of Google's decision and had no comment.

Was Bill Gates' Death-of-Spam Prediction Premature?

In January 2004, Bill Gates, the chairman of Microsoft, famously predicted the end of spam in a speech at the World Economic Forum. "Two years from now, spam will be solved," Gates said in his speech. But, as any e-mail user knows, spam is still flying over the Internet into everybody's inboxes.

"Spam is not dead, obviously, nor is it dying," said Forrester Research analyst Jonathan Penn. "But I do think that it is a problem that has been largely solved for end-users, employees, and consumers."

There are plenty of good antispam products from enterprise-security vendors as well as solutions developed by and deployed at Internet service providers (ISPs), according to Penn. "These are far from perfect, to be sure, but very good," he said.

"However, for ISPs especially, the spam problem is not fully solved by any means," Penn said. "They still spend a lot of money on R&D in a cat-and-mouse game with spammers, as well as the infrastructure investment to deal with the inbound volume that gets rejected at or near the gateway." In 2004, Microsoft came up with the concept of Sender ID, an e-mail authentication technology, as a means of combating spam. Sender ID checks a registered list to determine whether a message came from the same domain as the e-mail address indicates. The technology has not caught on among ISPs and corporations.

"Sender authentication solutions are very slow to reach maturity, and that is simply a shame on the ISPs, who have not been aggressive enough in developing the specs and deploying them in full force," Penn said. "In this case, the 'perfect' is the enemy of the 'good enough,'" Penn explained. "The world would not stop spinning if ISPs would implement effective, albeit imperfect, solutions available today. We've seen much more tolerance by companies for imperfect solutions - those that might temporarily block some e-marketing messages, for example - than the ISPs seem comfortable deploying."

Penn pointed out that, in addition to helping solve the spam problem, sender-authentication technologies can be useful for stopping phishing attacks. "These problems, especially phishing, have not even diminished,

much less gone away," Penn said.

Ken Schneider, chief architect at U.S. Internet security vendor Symantec, said that his company is generally supportive of e-mail-authentication efforts.

"These do not solve the problem of spam, but they provide an additional level of filtering on top of antispam filters," Schneider said. "You need very dynamic antispam filters, as the spam being sent out changes on a daily basis," Schneider pointed out. "But if e-mail users have a good antispam filter in their e-mail system, they should catch most of the spam. And if an ISP deploys effective filtering, they will block a lot of junk e-mails."

In recent months, there have been several high-profile U.S. court cases in which spammers have received heavy sentences.

On Monday, January 23, Jeanson James Ancheta, of Downey, California, pleaded guilty to federal charges related to his assembly of a botnet consisting of hundreds of thousands of computers to spread spam and malicious software, and of profiting from the zombie machines through the unauthorized distribution of adware.

Last month, CIS Internet Services, a Clinton, Iowa-based Internet service provider, was awarded $11.2 billion in a court judgment against a Florida man who sent millions of unsolicited pieces of commercial e-mail.

U.N. Lends Backing to the $100 Laptop

The United Nations on Thursday lent its support to a project which aims to ship inexpensive, hand-cranked laptops to school-aged children worldwide.

Kemal Dervis, head of the U.N. Development Program, will sign a memorandum of understanding Saturday with Nicholas Negroponte, chairman of One Laptop per Child, on the $100 laptop project, at the World Economic Forum’s annual meeting.

The program aims to ship 1 million units by the end of next year to sell to governments at cost for distribution to school children and teachers.

UNDP will work with Negroponte’s organization to deliver "technology and resources to targeted schools in the least developed countries," the U.N. agency said in a statement.

Negroponte wants to start shipping the cheap laptop, which is to have wireless network access and a hand-crank to provide electricity, later this year. The aim is to have governments or donors buy them and give full ownership to the children.

Negroponte, who is also chairman of the MIT Media Lab, has said he expects to sell 1 million of them to Brazil, Thailand, Egypt and Nigeria.

The laptop is expected to run on an open-source operating system, such as Linux.

The devices will be lime green in color, with a yellow hand crank, to make them appealing to children and, so the thinking goes, to fend off potential

thieves.

Free Lunch Ends for Most Electronic Filers

If you file your taxes online, your free lunch may be over.

Last year, anyone who filed their income taxes through the Internal Revenue Service could find a preparer who would do it free of charge through Free File, the IRS's online tax preparation program. This year, the IRS is closing the window to taxpayers who make more than $50,000. Depending on the service provider you choose - H&R Block, TurboTax, TaxAct or others - you may face lower income limits and even age requirements.

The main reason for the new cap is economic. When Free File started in 2003, most companies imposed income requirements, in line with the program's goal of helping lower-income people file their taxes electronically.

In an effort to gain market-share, however, many companies last year offered free filing to anyone, regardless of income. One was TurboTax, a product of Intuit Inc. Companies that started the filing season last year with income requirements - including H&R Block Inc. and OLT.com - lifted those requirements within a few days to compete.

"It became a free-for-all," said Denise Sposato, a spokeswoman with H&R Block.

"It had started looking like Free File was going to destroy the industry," said the IRS's Bert DuMars. DuMars, director of electronic tax administration, spent months discussing a possible solution with vendors before settling on the new income requirements.

The new $50,000 income cap will be adjusted annually. The main goal is that Free File services 70 percent of the taxpayer population; this year, that represents anyone with an income of $50,000 or less, DuMars said.

Companies are also setting their own limits within the broader IRS guidelines. H&R Block is providing the service to people with an income of $50,000 or less, and with an age restriction of 50 and under. TurboTax is only providing the free filing services to people with an adjusted gross income of no more than $28,500, or for people who were on active military duty in 2005 with income of no more than $50,000.

Refund anticipation loans, which are high interest-rate loans of taxpayers' refund amounts, also face new requirements: Companies must provide upfront disclosure fees and interests rates. One reason tax preparers had been willing to offer free filing services in part was because they hoped to make up revenue by cross-selling other products and services, like financial planning, mortgages or refund anticipation loans.

Whether you qualify for Free File or not, be sure to shop around for the provider that best suits your needs. This year, the IRS expects 21 companies to join its growing list of providers, which can be found at the IRS web site: http://www.irs.gov.

Here are some pointers to consider:

* What does it cost: Filing online is still one of the cheapest ways to file taxes. Those who aren't eligible for Free File should be prepared to spend between $25 and $35 for both federal and state tax returns. If you are eligible for Free File, you want to be sure you can also file your state taxes in the same place. Also, be sure to check the fees associated with filing a state tax return since it usually isn't free.

* Can you take your time? When choosing an online tax preparer, you want to make sure you take as long as you need, coming back as often as you need. It can be impossible to finish your taxes in one sitting, so you want to be able to save your unfinished work.

* Can you get help? Before choosing an online filing program, make sure it has the options you prefer for contacting someone if you need assistance. Some programs offer no telephone number, for example, so people who feel most comfortable talking to a real person want to make sure a call center is available.

EU Extends Microsoft Antitrust Deadline

The European Commission has agreed to extend a deadline for Microsoft Corp. to provide better documentation so its software programs can be used with competitors' products, the company said Tuesday.

Microsoft spokesman Dirk Delmartino said EU regulators had given the company until Feb. 15 to answer a complaint that it is still failing to obey the 2004 antitrust ruling.

"We wanted the time to study and respond to it. It arrived just before the holidays," he said.

Last month, the EU executive threatened to fine Microsoft up to 2 million euros ($2.36 million) a day backdated to Dec. 15, saying the company was proving intransigent about sharing data with competitors.

Microsoft retorted that the EU Commission was trying to undermine its Windows operating system with ever-more-drastic demands for technological transparency, and that it would contest the measure under EU law.

The company claims that the commission's latest demands on opening up its software specifications would also open the door to the cloning of the company's core product, the ubiquitous Windows operating system.

EU regulators based the decision on a report from the monitoring trustee of the 2004 agreement which said Microsoft's concessions were insufficient so far.

"Any programmer or programming team seeking to use the technical documentation for a real development exercise would be wholly and completely unable to proceed on the basis of the documentation. The technical documentation is therefore totally unfit at this stage for its intended purpose," the report by British computer scientist Neil Barrett said.

The EU ordered Microsoft in March 2004 to pay 497 million euros ($613 million), share code with rivals and offer an unbundled version of Windows without the Media Player software for what it saw as an abuse of its

dominant position in the industry. The Court of First Instance, the EU's second-highest court, has not yet set a date to hear Microsoft's appeal.

=~=~=~=

Atari Online News, Etc. is a weekly publication covering the entire Atari community. Reprint permission is granted, unless otherwise noted at the beginning of any article, to Atari user groups and not for profit publications only under the following terms: articles must remain unedited and include the issue number and author at the top of each article reprinted. Other reprints granted upon approval of request. Send requests to: dpj@atarinews.org

No issue of Atari Online News, Etc. may be included on any commercial media, nor uploaded or transmitted to any commercial online service or internet site, in whole or in part, by any agent or means, without the expressed consent or permission from the Publisher or Editor of Atari Online News, Etc.

Opinions presented herein are those of the individual authors and do not necessarily reflect those of the staff, or of the publishers. All material herein is believed to be accurate at the time of publishing.